



# License Manager User Manual

# Table of Contents

---

Overview .....	3
My Casino Accounts .....	5
<b>Logging into MCA (www.mycasinoaccounts.com).....</b>	<b>5</b>
<b>Logging out of MCA (www.mycasinoaccounts.com).....</b>	<b>5</b>
Accounts License Manager System .....	5
<b>Accessing the License Manager System .....</b>	<b>5</b>
Wiping .....	6
<b>About Wiping .....</b>	<b>6</b>
<b>What to do if the Casino is not working .....</b>	<b>6</b>
Register Site .....	7
<b>Registering a Site .....</b>	<b>7</b>
Activate Site .....	7
<b>Activating a Site .....</b>	<b>7</b>
Manage Site .....	8
<b>Managing a Site .....</b>	<b>8</b>
<b>Status Descriptions .....</b>	<b>10</b>
User Manuals .....	12
Appendix 1 – Reason Codes that May Trigger an Internal Wipe Process .....	13
Appendix 2 – Events that will Cause BitLocker to Enter Recovery Mode When Attempting to Start the Operating System Drive.....	14

# Overview

---

The RTG Stand Alone Casino is a casino solution which can be deployed to locations (Cafes) where Internet connections have a non-reliable or intermittent behavior.

The solution requires the installation of a local server on every Cafe making the system resilient to internet communication failures.

To mitigate security risks associated with the nature of this product, local servers include special processes for license installation, site registration, site activation and even automatic/ manual site wiping.

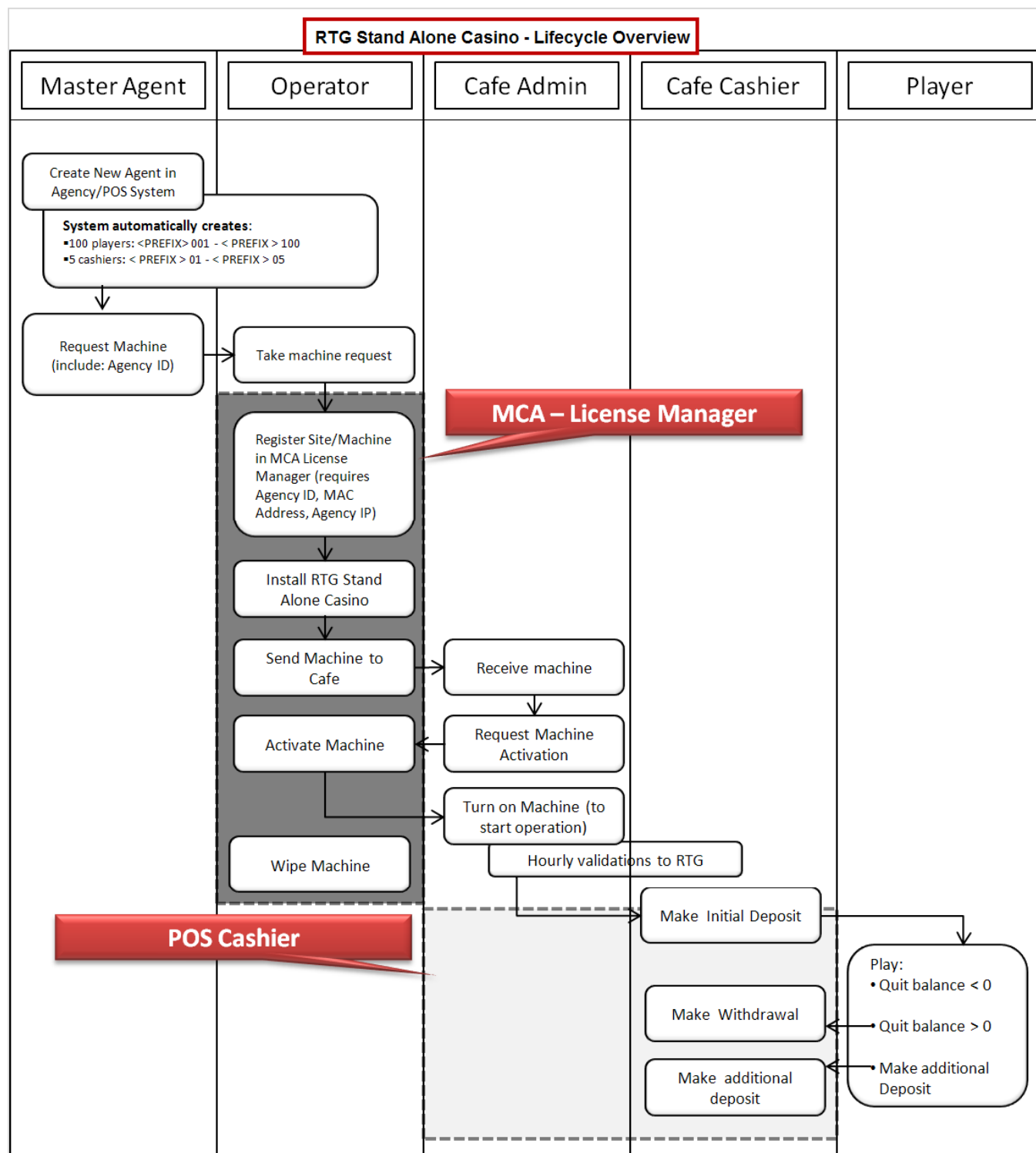
To set up and run the RTG Stand Alone Casino, follow these steps:

1. **Create New Agent and Request Machine** – the Master Agent (in some casinos the Master Agent and Operator roles are taken on by the same person) creates a new agent in the Agency/ POS system. As soon as the new agent is created, the system automatically creates :
  - 100 players, using the following naming format: <PREFIX> 001 – <PREFIX> 100<sup>1</sup>
  - 5 cashiers, using the following naming format: <PREFIX> 01 – <PREFIX> 05Then, the Master Agent sends the Operator a request for a machine. This request must include the Agency ID.
2. **Take Machine Request and Prepare the Machine** – the Casino Operator
  - receives the request for a machine form the Master Agent
  - prepares the machine (Server)
  - registers the machine in the MCA License Manager – which will require: the Agency ID, and the MAC Address  
NOTE: Below in this MCA License Manager User Manual, there is detailed information on how to register a machine.
  - Installs the RTG Stand Alone Casino in the machine
  - Sends machine to Café
3. **Receive Machine and Request Activation** – the Cafe Administrator requests the installed machine, and requests activation of said machine to the Operator. This is critical because turning on a machine which has not been activated will automatically trigger a machine-wiping process.
4. **Activate Machine** – the Casino Operator
  - activates the machine in the MCA License Manager  
NOTE: Below in this MCA License Manager User Manual, there is detailed information on how to activate a machine.
  - informs Cafe Administrator that machine has been activated
5. **Turn on Machine** – the Cafe Administrator, making sure there is an online connection, turns on the machine for the first time. Assuring there is an online connection is critical because turning on a machine for the first time without an internet connection will automatically trigger a machine wiping process.
6. **Manage Cashiers** – the Cafe Administrator, can change the passwords of the five cashiers (created in step one above) in the RTG Stand Alone Casino
7. **Manage Cafe** – the Cafe Cashier can manage the Cafe which implies making deposits into player's account, making withdrawals out of a player's account, and changing player's passwords.

---

<sup>1</sup> The prefix is defined by the system

The chart below shows the process in more detail:



## My Casino Accounts

### Logging into MCA ([www.mycasinoaccounts.com](http://www.mycasinoaccounts.com))

To Log into MCA, follow these steps:

1. Go to <https://www.mycasinoaccounts.com>
2. Type your login name into the **RSA UserName** box (*supplied to you*)
3. Type your password into the **RSA PASSCODE** box (*supplied to you*)
4. Press the **Submit** button.

### Logging out of MCA ([www.mycasinoaccounts.com](http://www.mycasinoaccounts.com))

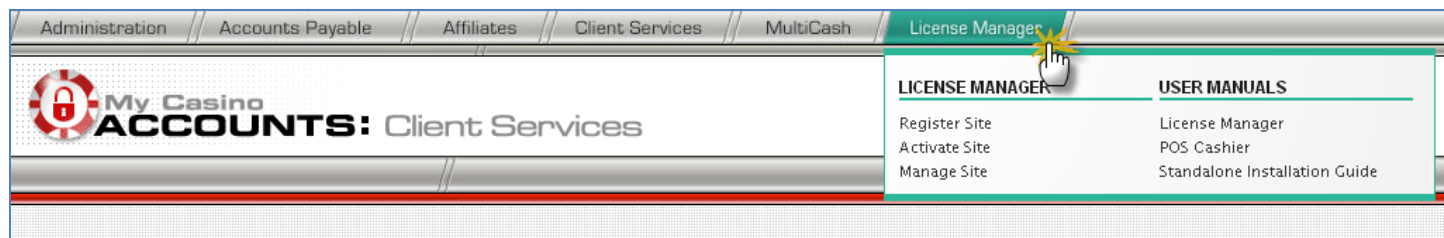
- To Log out of MCA, click the Log Out button, on the upper right side of screen

## Accounts License Manager System

### Accessing the License Manager System

To Access the License Manager System in MCA, follow these steps:

- Once you are logged in MCA, point to the License Manager menu item in the Horizontal MCA Menu at the top. As soon as you hover the mouse pointer over the License Manager option, the License Manager menu will drop down.



# Wiping

## About Wiping

Wiping, a process that overwrites the Site data rendering it unusable, can be triggered:

- manually from the Manage Site page in MCA; or
- automatically if:
  - the Stand Alone Site (Server) is turned on for the first time without an internet connection (remember that turning on the Stand Alone Site (Server) – once installed, yet not activated – will also trigger the wiping process),
  - the logged data is proven invalid at various checkpoints,
  - tampering is suspected, or
  - the Stand Alone Site (Server) is offline<sup>2</sup> for over 24 hours<sup>3</sup>.



**WARNING:** Wiping will result in the loss of all data in Stand Alone Site (Server) and which has not been backed up.

## What to do if the Casino is not working

If the POS cashier page or the casino games is not working, then, the server has likely been wiped, either manually or automatically. Regardless of the reason that triggered the wiping on the Stand Alone Site (Server), and if you wish to restart operations, contact your Operator both to report the problem and get the delivery time for the replacement equipment.



### **WARNING**

- After wiping, the only solution to restart operations is a machine replacement.

<sup>2</sup> In this User Manual, the term **offline** refers to being disconnected from the Internet.

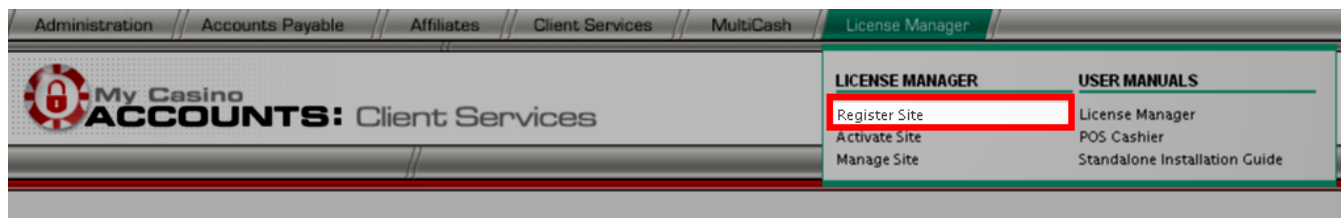
<sup>3</sup> This time length may be modified. Double-check with your Operator.

# Register Site

## Registering a Site

A Site which will be used to host a Stand-Alone Casino must be registered into MCA before the RTG Casino can be installed thereon. To register a Site in MCA, follow these steps:

1. From the License Manger drop-down menu, select **Register Site**.



2. In the Register Site page, complete the required fields:

- **Name** – Name that identifies the Site
- **MAC Address** – The Media Access Control address (MAC address) is the physical ID of the Site's network interface card. This address must be registered before installing the Site Server for a Cafe because it will be used by the Site Installer to report installation to the License Server. MAC address must be used in the XX:XX:XX:XX:XX:XX format.



**WARNING:** If a Site is not registered when the installation process finishes, an automatic wipe action will be triggered.

- **External ID** – Unique identifier assigned to the Site

3. Then, click the **Save** button.

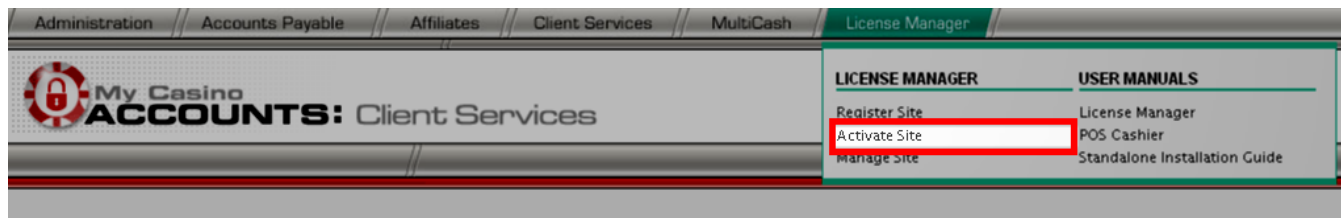
NOTE: If you click the **Cancel** button, all data entered will be cleared from the fields.

# Activate Site

## Activating a Site

A Site must be registered and installed before it can be activated. To activate a Site, follow these steps:

1. From the License Manager drop-down menu, select **Activate Site**.



2. In the Activate Site page, enter the External ID of the Site you wish to activate.

NOTE: If has not been installed, it will not be displayed and the system will report "item not found".

3. Click the **Activate Link** option.

NOTE: Once activated, a Site will be hourly<sup>4</sup> validated by RTG.

A Site's first activation required an online connection or an automatic wiping process will be triggered.

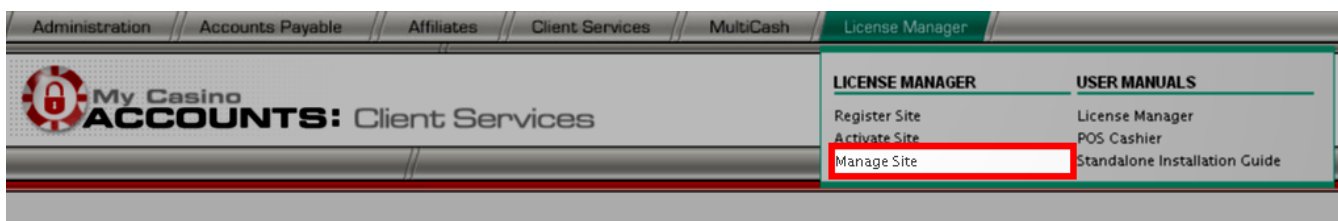
To avoid automatic Site wiping, make sure to have internet connection for the Site's first power-on after activation.

## Manage Site

### Managing a Site

To manage your Site(s), follow these steps:

1. From the License Manager drop-down menu, select **Manage Site**.



2. In the Manage Site page, enter the desired search criterion(a) – either one search criterion or a combination thereof to narrow down the search.

SEARCH CRITERIA	
<b>External ID</b>	<p>Unique identifier assigned to the Site obtained from the Agency System.</p> <p>This value is going to be the ID of the machine and will be used as prefix to create the default set of player accounts during installation.</p>
<b>MCA Address</b>	<p>The Media Access Control address (MAC address) is the physical ID of the Site's network interface card.</p> <p>This address must be registered before installing the Site Server for a café because it will be used by the Site Installer to report installation to the License Server.</p> <p>If a Site is not registered when the installation process finishes, an automatic wipe action will be triggered.</p>
<b>Name</b>	Name that identifies the Site
<b>Status</b>	See status descriptions section below

<sup>4</sup> This time length may be modified. Double-check with your Operator.



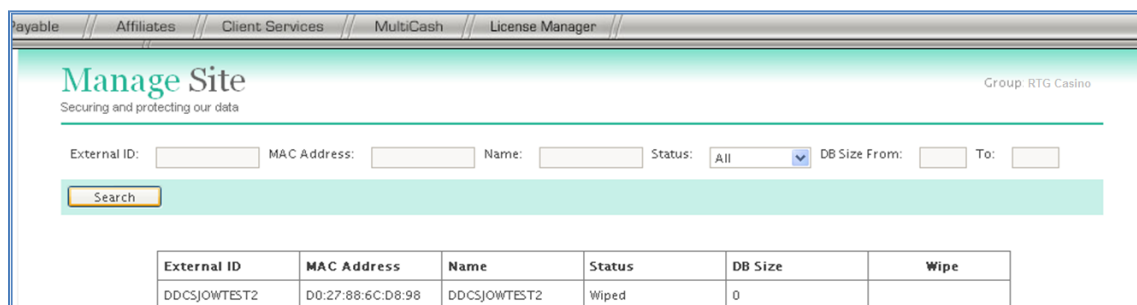
### DB Size

Indicates the actual database usage in MB. It must be entered as a range.

TIP – Use to monitor which DBs may be approaching their maximum capacity.

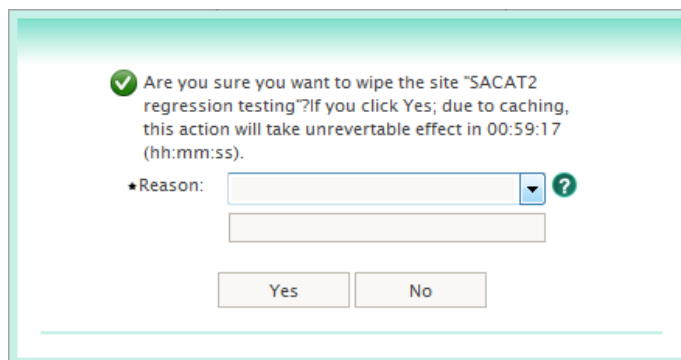
Click the **Search** button, and the System will generate a list with the Site(s) that matches your predefined criteria.

**NOTE:** If you click Search without entering any information (External ID, MAC Address, Status, DB Size), the System will generate a list of all your sites.



External ID	MAC Address	Name	Status	DB Size	Wipe
DDSCJOWTEST2	D0:27:88:6C:D8:98	DDSCJOWTEST2	Wiped	0	

- To wipe a Site, click the Wipe link.



- On the pop-up message, select a reason from the drop-down<sup>5</sup> (damage, stolen). Then, click the Yes button.

**NOTE:** Clicking Yes will trigger a wiping action which will overwrite the Site's (server) data rendering unreadable in the time lapse displayed, which is the only time window for reverting the action.

After clicking Yes, the status of the Site will automatically change to Wipe Requested.

If you click the **Cancel** button, all data entered will be cleared, and the system will take you back to the Manage Site page.

<sup>5</sup> Selecting "Other" will require a reason to be specified.

## Status Descriptions

Sites in the system are assigned one of the following statuses:

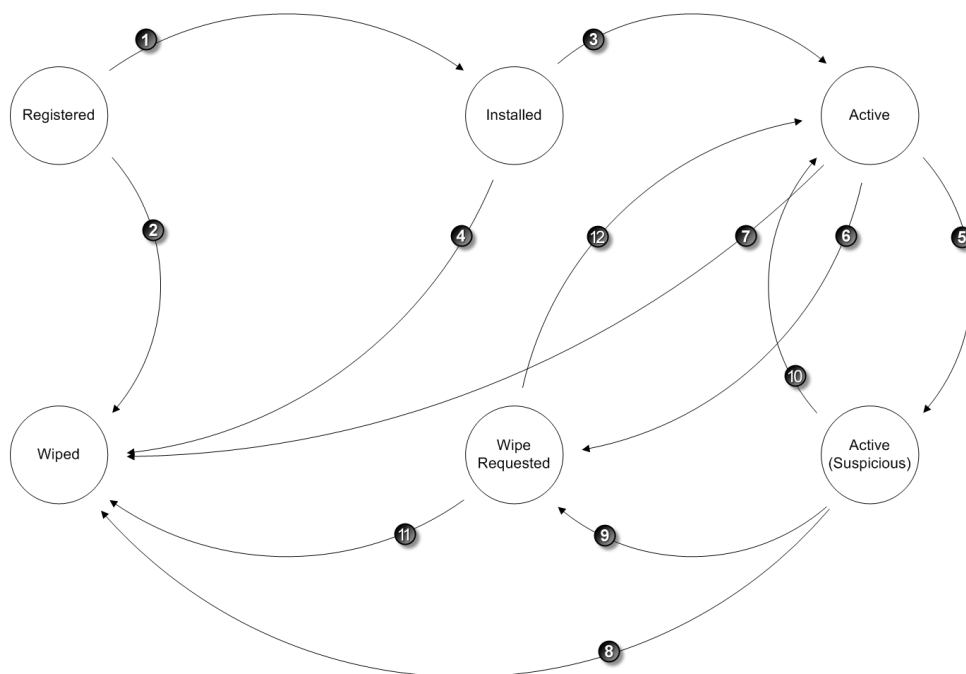
Status	Description
Registered	Indicates the Site is already registered, but not installed. Not ready to go live.
Installed	Indicates the Site is ready for activation.
Activated	Indicates the Site is in working order
Activated (Suspicious)	<p>Indicates the Site is active, but last validation to RTG did not happen when expected, and it is still pending.</p> <p>This status indicates something is interfering with the regular Site validation, or even Site theft or seizure.</p> <p>Sites can hold this status for 24 hours<sup>6</sup> maximum, before an automatic wipe is triggered.</p>
Wipe Requested	<p>Indicates the Site will be wiped once validation time is over.</p> <p>Maximum validation time is 1 hour, before an automatic wipe is triggered.</p> <p>Wiping for a Site displaying this status may still be reverted.</p>
Wiped	<p>Indicates the Site was wiped manually or automatically. Automatic Wipes are triggered at predefined security compromising conditions.</p> <p>For more information on automatic wiping triggers, see the About Wiping section above.</p>

The following page shows changes from one status to another both graphically in diagram and explained in a chart.

---

<sup>6</sup> This time length may be modified. Double-check with your Operator.

Changes from one status to another are shown in the image below, and explained in the chart that follows:

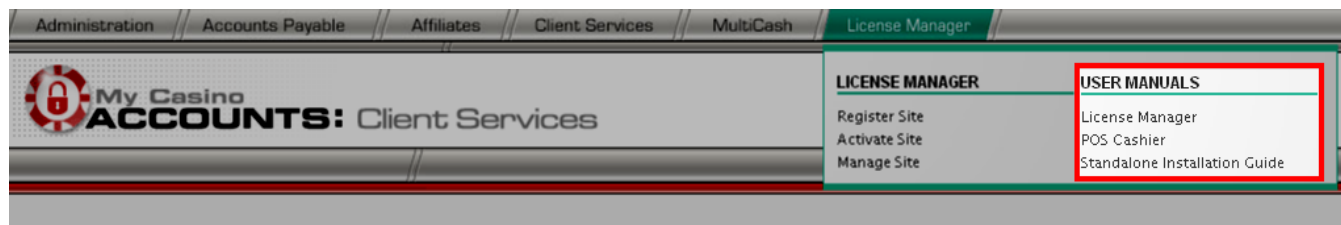


IF Site status is	and the action below happens	Site status changes to
1. Registered	RTG Stand Alone Casino is installed in Stand Alone Site (Server)	Installed
2. Registered	A wipe process is manually requested in MCA	Wiped
3. Installed	Installed Site is activated in MCA	Active
4. Installed	a) Site is not activated before first power-on b) A wipe process is manually requested in MCA	Wiped
5. Active	Regular communication between Site and License Server is interrupted.	Active (Suspicious)
6. Active	A wipe process is manually requested in MCA	Wipe Requested
7. Active	a) Site (Server) is turned on for the first time without an internet connection b) the logged data is proven invalid at any of the various checkpoints c) tampering is suspected d) the Stand Alone Site (Server) is offline for over 24 hours	Wiped
8. Active (Suspicious)	If this status is kept for over 24 hours	Wiped
9. Active (Suspicious)	A wipe process is manually requested in MCA	Wipe Requested
10. Active (Suspicious)	Regular communication between Site and License Server is re-established.	Active
11. Wipe Requested	A system defined period of time (between wiping request and actual wiping action) lapses	Wiped
12. Wipe Requested	A Wipe Requested is reverted by cancelling it in MCA	Active

# User Manuals

There are three manuals available in PDF format:

- License Manager
- POS Cashier
- StandAlone Installation Guide



To view a manual, click the corresponding on the link in the License Manager drop-down menu.

## Appendix 1 – Reason Codes that May Trigger an Internal Wipe Process

Code ID	Description	Comments
10100	The security policy is not set according installation process	Something has changed in Windows security policies, which is not permitted.
10200	There are users logged in during the token validation process	Nobody can log in after the casino has been installed and the machine has been rebooted.
10300	The CD is enable on windows	DVD or CD drives are disabled by the installation process. If for some reason they become active again, tampering may be underway and this triggers the wipe.
10400	The USB are enabled on windows	Same rule applied to CD and DVD, but only affects USB storage devices. USB keyboard and mouse are permitted.
10500	The TMP device is not installed	
10600	Drive D is not configured according installation process	Drive D must have a determined size and configuration. If the system detects changes there, it wipes.
10700	Drives are not encrypted using BitLocker	
10800	The date or time on the machine was changed	Wipe gets activated if PC's internal clock gets fast or slow for 10 minutes or more, with respect to the clock of the License Server (this clock is synchronized with a global server).
10900	The token expired	
11000	The license server response is "Wipe"	Wipe was manually requested from the administration page of the License Server, in MCA.
11100	The prerequisite application is not valid	Some components used for executing security checks are missing.
11200	The casino GUID is not valid	The GUID of the machine couldn't be read from the Registry.
11300	Maximum number of retries reached during the first token validation	The first time the machine is rebooted after casino installation, the system requests the first token to the License Server. If no response is received, it retries every minute, for up to 30 minutes. If no valid token has been received after 30 minutes, the system self-destructs.
10071	Security policy execution fail	These codes are used when, for some reason, one of the above validations (10100 to 11300) raises an exception during execution. The system assumes that something is trying to prevent validations, so it triggers the wipe.
10072	Users logged validation fail	
10073	CD disable validation fail	
10074	USB disable validation fail	
10075	TMP installed validation fail	
10076	Drive D configuration fail	
10077	Drives encrypted validation fail	
10078	Apply firewall rules fail	

# Appendix 2 – Events that will Cause BitLocker to Enter Recovery Mode When Attempting to Start the Operating System Drive

Taken from: [http://technet.microsoft.com/en-us/library/ee449438\(WS.10\).aspx#BKMK\\_examplesosrec](http://technet.microsoft.com/en-us/library/ee449438(WS.10).aspx#BKMK_examplesosrec)

## What causes BitLocker to start into recovery mode when attempting to start the operating system drive?

The following list provides examples of specific events that will cause BitLocker to enter recovery mode when attempting to start the operating system drive:

- Changing any boot configuration data (BCD) boot entry data type settings with the exception of the following items:

DESCRIPTION

RAMDISKIMAGEOFFSET

PASSCOUNT

TESTMIX

FAILURECOUNT

TESTTOFAIL

### Warning

When installing a language pack, an additional option in the language pack installation wizard asks if the user wants to apply language settings to **All users and system accounts**. If this option is selected, it will change the local computer BCD settings (if the user-only option is selected, BCD settings are not changed). This change will result in a modification of a BCD setting to the new locale value. If you are using a TPM with BitLocker, this is interpreted as a boot attack on reboot and the computer will require that the user enter the recovery password or recovery key to start the computer.

We recommend that you suspend BitLocker before changing locales or installing a language pack, just as you would before making any major computer configuration change, such as updating the BIOS.

- Changing the BIOS boot order to boot another drive in advance of the hard drive.
- Having the CD or DVD drive before the hard drive in the BIOS boot order and then inserting or removing a CD or DVD.
- Failing to boot from a network drive before booting from the hard drive.
- Docking or undocking a portable computer. In some instances (depending on the computer manufacturer and the BIOS), the docking condition of the portable computer is part of the system measurement and must be consistent to validate the system status and unlock BitLocker. This means that if a portable computer is connected to its docking station when BitLocker is turned on, then it might also need to be connected to the docking station when

it is unlocked. Conversely, if a portable computer is not connected to its docking station when BitLocker is turned on, then it might need to be disconnected from the docking station when it is unlocked.

- Changes to the NTFS partition table on the disk including creating, deleting, or resizing a primary partition.
- Entering the personal identification number (PIN) incorrectly too many times so that the anti-hammering logic of the TPM is activated. Anti-hammering logic is software or hardware methods that increase the difficulty and cost of a brute force attack on a PIN by not accepting PIN entries until after a certain amount of time has passed.
- Turning off the BIOS support for reading the USB device in the pre-boot environment if you are using USB-based keys instead of a TPM.
- Turning off, disabling, deactivating, or clearing the TPM.
- Upgrading critical early startup components, such as a BIOS upgrade, causing the BIOS measurements to change.
- Forgetting the PIN when PIN authentication has been enabled.
- Updating option ROM firmware.
- Upgrading TPM firmware.
- Adding or removing hardware. For example, inserting a new card in the computer, including some PCMCIA wireless cards.
- Removing, inserting, or completely depleting the charge on a smart battery on a portable computer.
- Changes to the master boot record on the disk.
- Changes to the boot manager on the disk.
- Hiding the TPM from the operating system. Some BIOS settings can be used to prevent the enumeration of the TPM to the operating system. When implemented, this option can make the TPM hidden from the operating system. When the TPM is hidden, BIOS secure startup is disabled, and the TPM does not respond to commands from any software.
- Using a different keyboard that does not correctly enter the PIN or whose keyboard map does not match the keyboard map assumed by the pre-boot environment. This can prevent the entry of enhanced PINs.
- Modifying the Platform Configuration Registers (PCRs) used by the TPM validation profile. For example, including PCR[1] would result in most changes to BIOS settings, causing BitLocker to enter recovery mode.

**Note**

Some computers have BIOS settings that skip measurements to certain PCRs, such as **PCR[2]**. Changing this setting in the BIOS would cause BitLocker to enter recovery mode because the PCR measurement will be different.

- Moving the BitLocker-protected drive into a new computer.
- Upgrading the motherboard to a new one with a new TPM.
- Losing the USB flash drive containing the startup key when startup key authentication has been enabled.

- Failing the TPM self test.
- Having a BIOS or an option ROM component that is not compliant with the relevant Trusted Computing Group standards for a client computer. For example, a non-compliant implementation may record volatile data (such as time) in the TPM measurements, causing different measurements on each startup and causing BitLocker to start in recovery mode.
- Changing the usage authorization for the storage root key of the TPM to a non-zero value.

**Note**

The BitLocker TPM initialization process sets the usage authorization value to zero, so another user or process must explicitly have changed this value.

- Disabling the code integrity check or enabling test signing on Windows Boot Manager (Bootmgr).
- Pressing the F8 or F10 key during the boot process.
- Adding or removing add-in cards (such as video or network cards), or upgrading firmware on add-in cards.
- Using a BIOS hot key during the boot process to change the boot order to something other than the hard drive.